Security Metrics Progression

Joshua Bartolomie
Director, Cyber Security Architecture
Exelis

Matthew Shaffer
Consultant, Strategic Solutions
Mandiant

Briefing Structure and Goals

- Framework and Planning
  - Matthew Shaffer – Strategic Solutions Consultant, Mandiant
- Implementation and Utilization
  - Joshua Bartolomie – Director, Cyber Security Architecture, Exelis Inc.

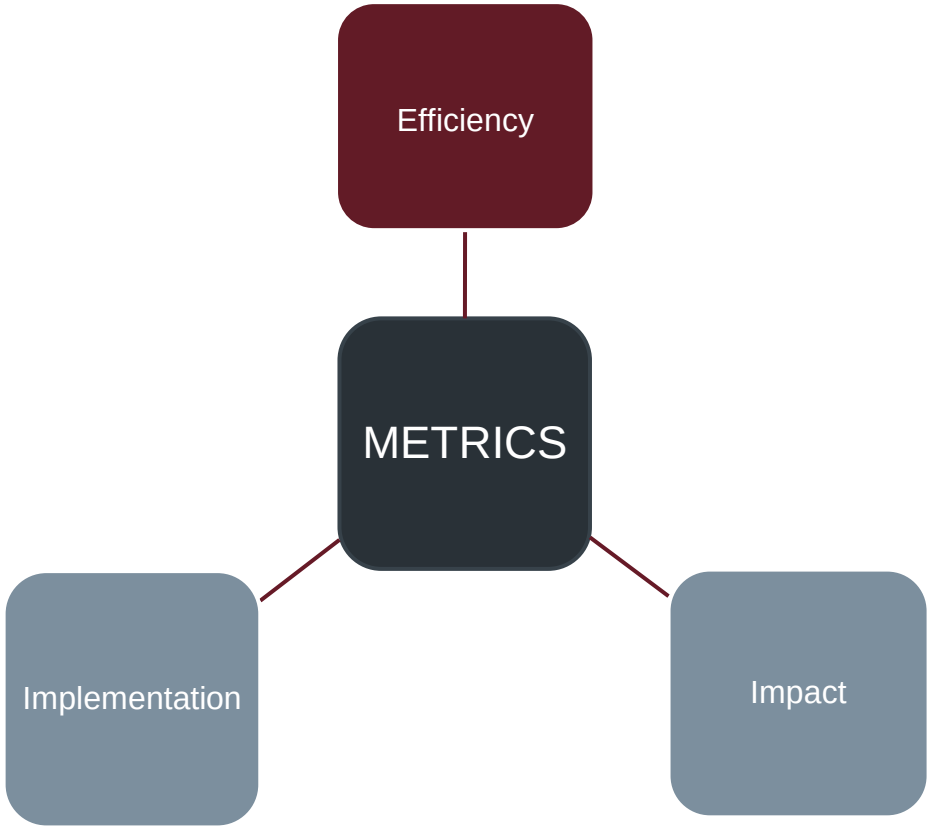
MIRcon 2013

Metrics Categories

**NIST SP 800-55 Rev. 1*

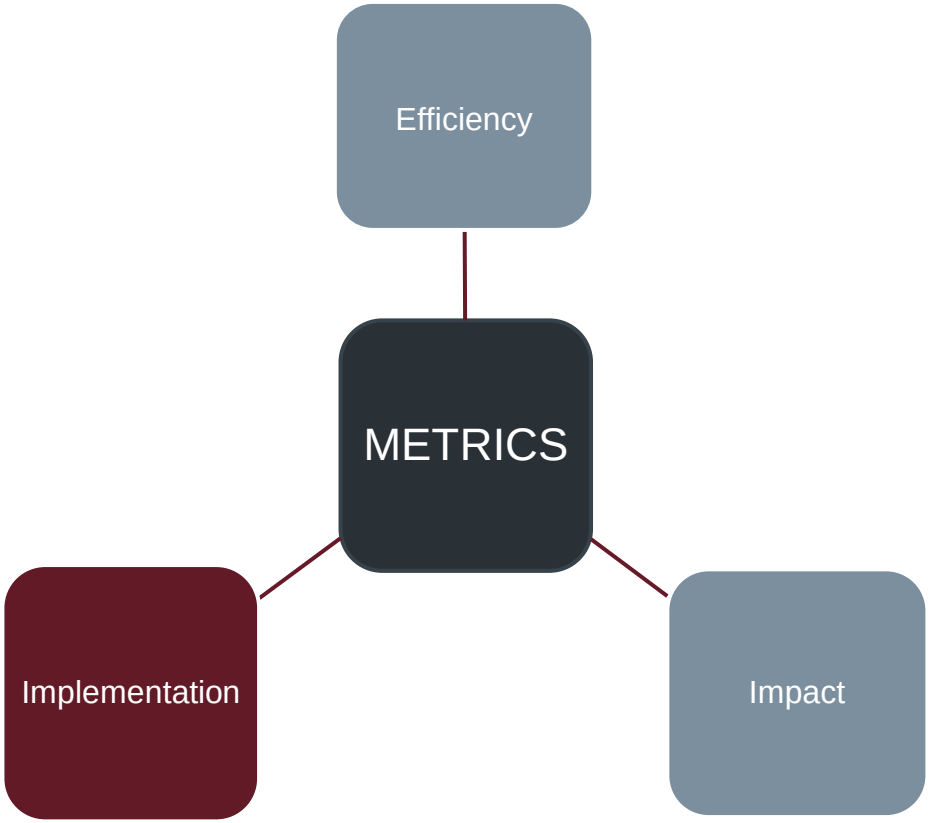
Efficiency Metrics

- Calculates effectiveness of monitoring and IR related people, process, and technology
- Typically CIRT internal
- Ex:
  - IR cycle time
  - # of incidents stopped by AV
  - DRAIN CVR



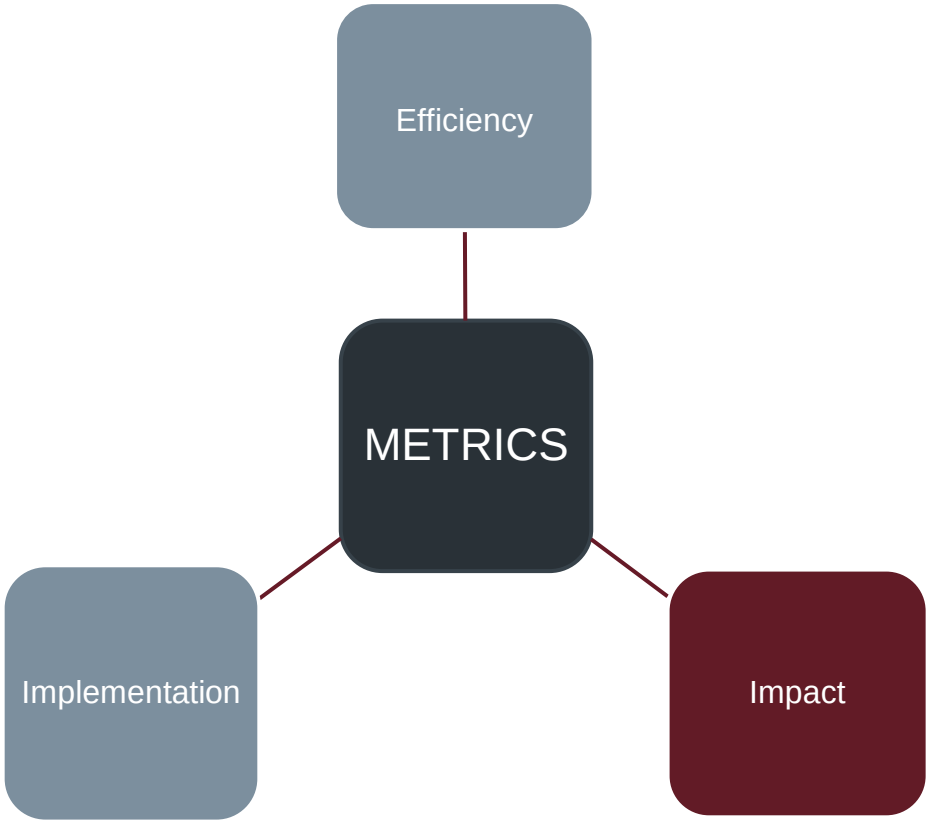
Implementation Metrics

- Calculates the progress of introducing new monitoring and IR related people, process, and technology
- Internally or externally focused
- Ex: Tracking successful technology deployment
  - % of web servers with new web application firewall
  - % of hosts with a given agent deployed



Impact Metrics

- Calculates the impact that the CIRT has on the business
- Externally focused
- May utilize results of other metrics
- Ex: real dollar value in the percentage decrease in time to detect since management approved the budget for an additional full time analyst



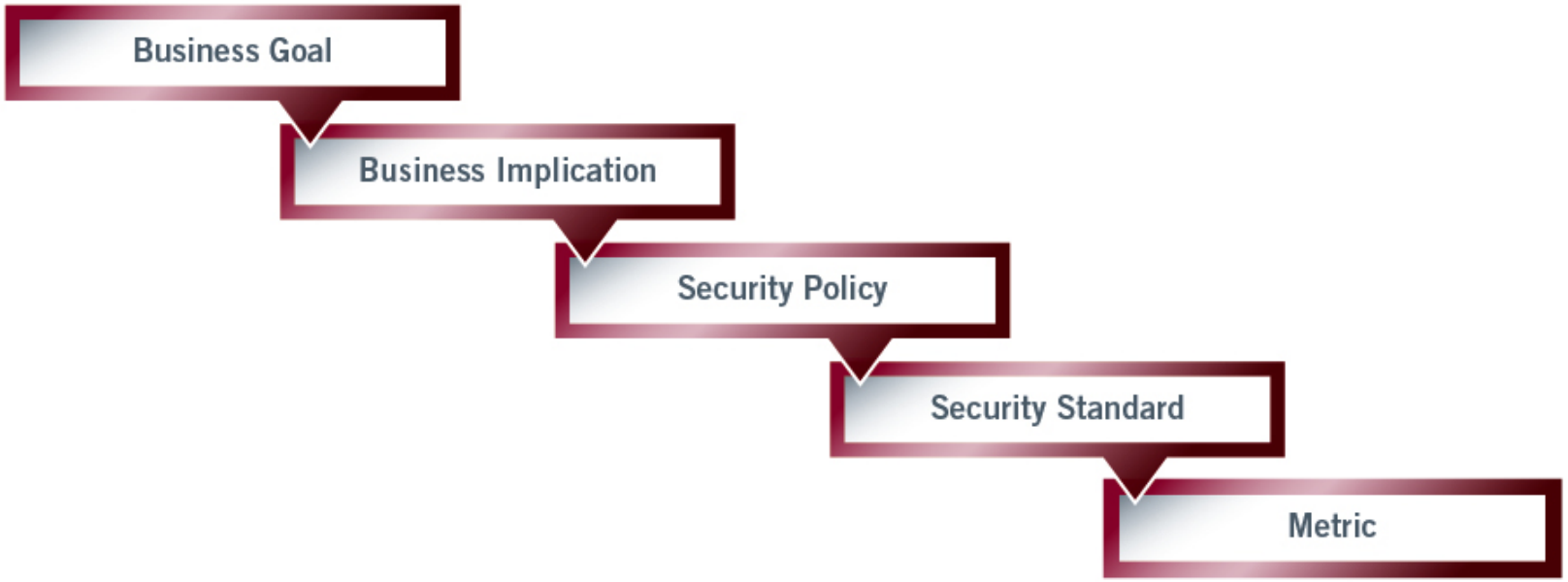
Proxy Metrics

- Use “proxy metrics” that are easily gathered in order to measure the hard-to-measure things you care about

You might not care about…	…but it’s a good way to measure
# of AV alerts per PC	Overall hygiene of environment
% of rogue/non-managed PCs on the network	Control over environment; prevalence of BYOD
Measuring every MS patch	Control over environment

Determining What to Measure

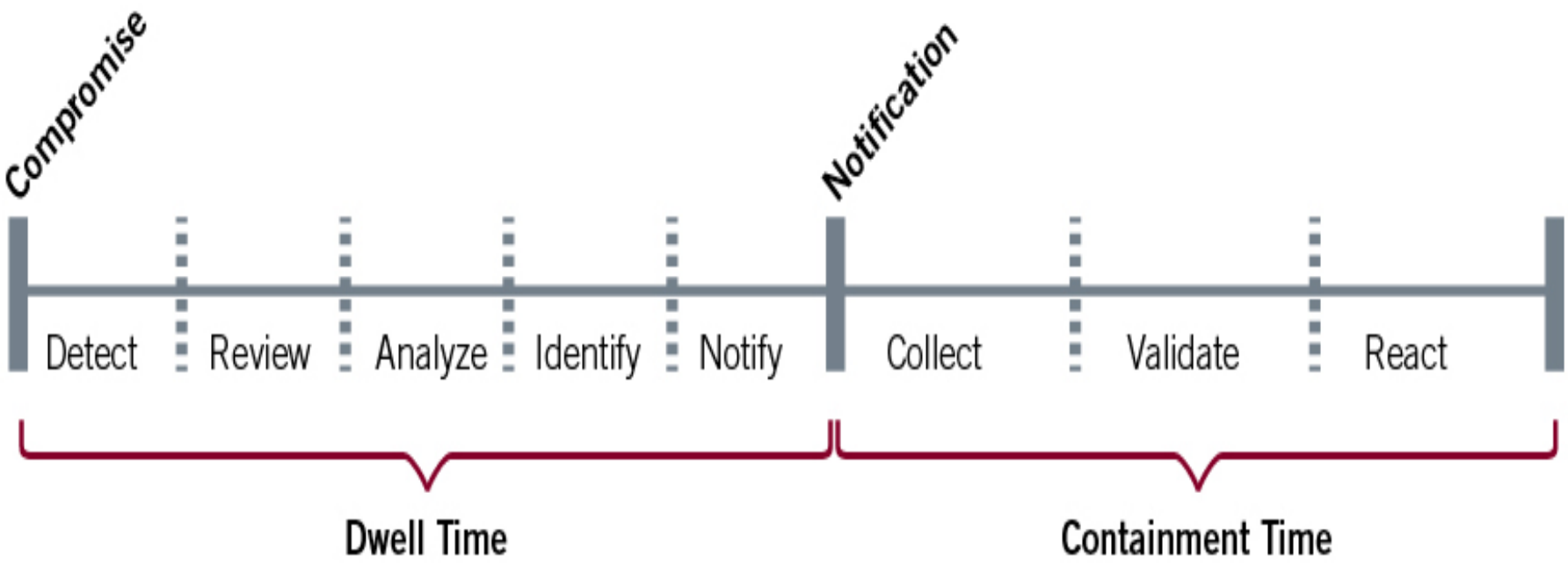
- Quantifiable
- Flow requirements downhill
- Consider a focus rotation



Requirements Flow

Source	Statement	
Business Goal	"To be the #1 credit card provider in the country"	How?
Business Implication	"We must maintain consumer trust"	How?
Security Policy	"All applications must adhere to Software Security Standards"	How?
Security Standard	"All input from web applications must be properly validated per this spec"	How?
Metric	"% of applications found to be vulnerable to SQL injection"	

DRAIN CVR - [dreyn kuhv-er] *noun.*



$$f((D + R + A + I + N) + (C + V + R))$$

DRAIN & CVR Defined

DRAIN CVR

Time	Category	Measurement	Benefit
Dwell	**Detect**	Time from initial entry into the system/network to detection	Measures the effectiveness of detection systems and capabilities
	Review	Time from detection to analyst to review the incident	Determine if staffing level is properly sized
	Analyze	Time to analyze the incident	Determines if the organization has the right expertise and tools and if the right escalation occurs
	Identify	Time to identify the affected assets, location, and owner	Measures the effectiveness of asset inventory
	Notify	Time to successfully notify appropriate contacts	Measures the effectiveness of contact database and communication plan
Containment	**Collect**	Time to collect live response data	Determines if there are the right tools deployed to assist in collection
	Validate	Time to validate intrusion based on collected data	Determines if the right skill sets are in place at each level
	React	Time to react (contain, remove, etc.)	Determines if there is the right definition of remediation and if it is applied consistently

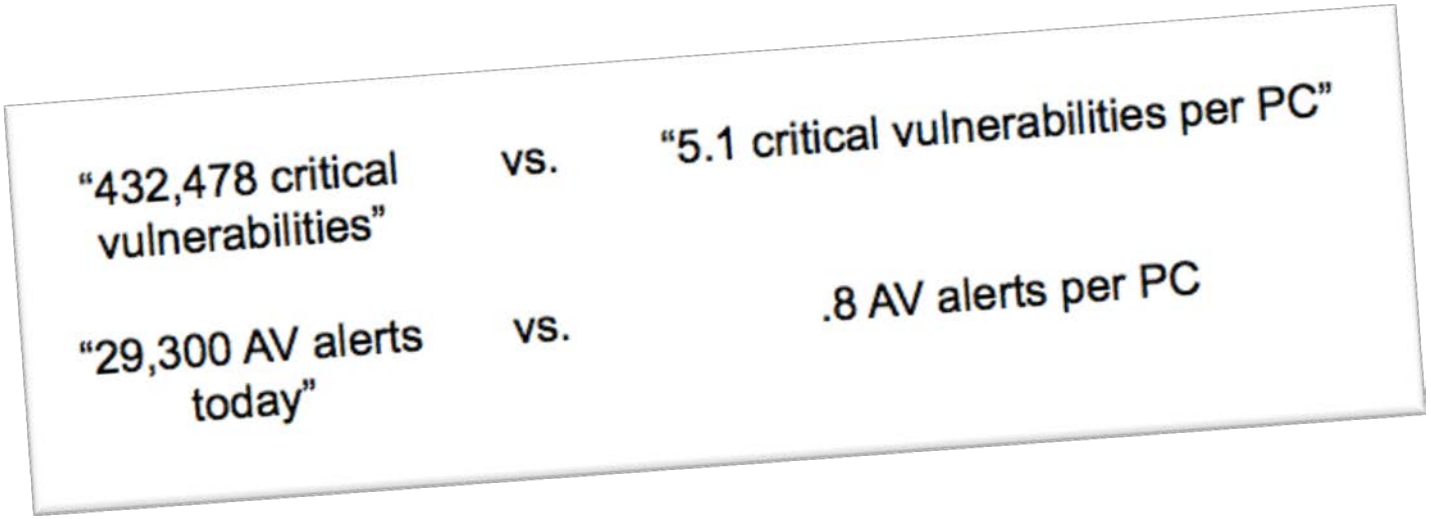
Reporting Template

- Documented and repeatable process
- Mission driven
- Consistent collection
- Communication

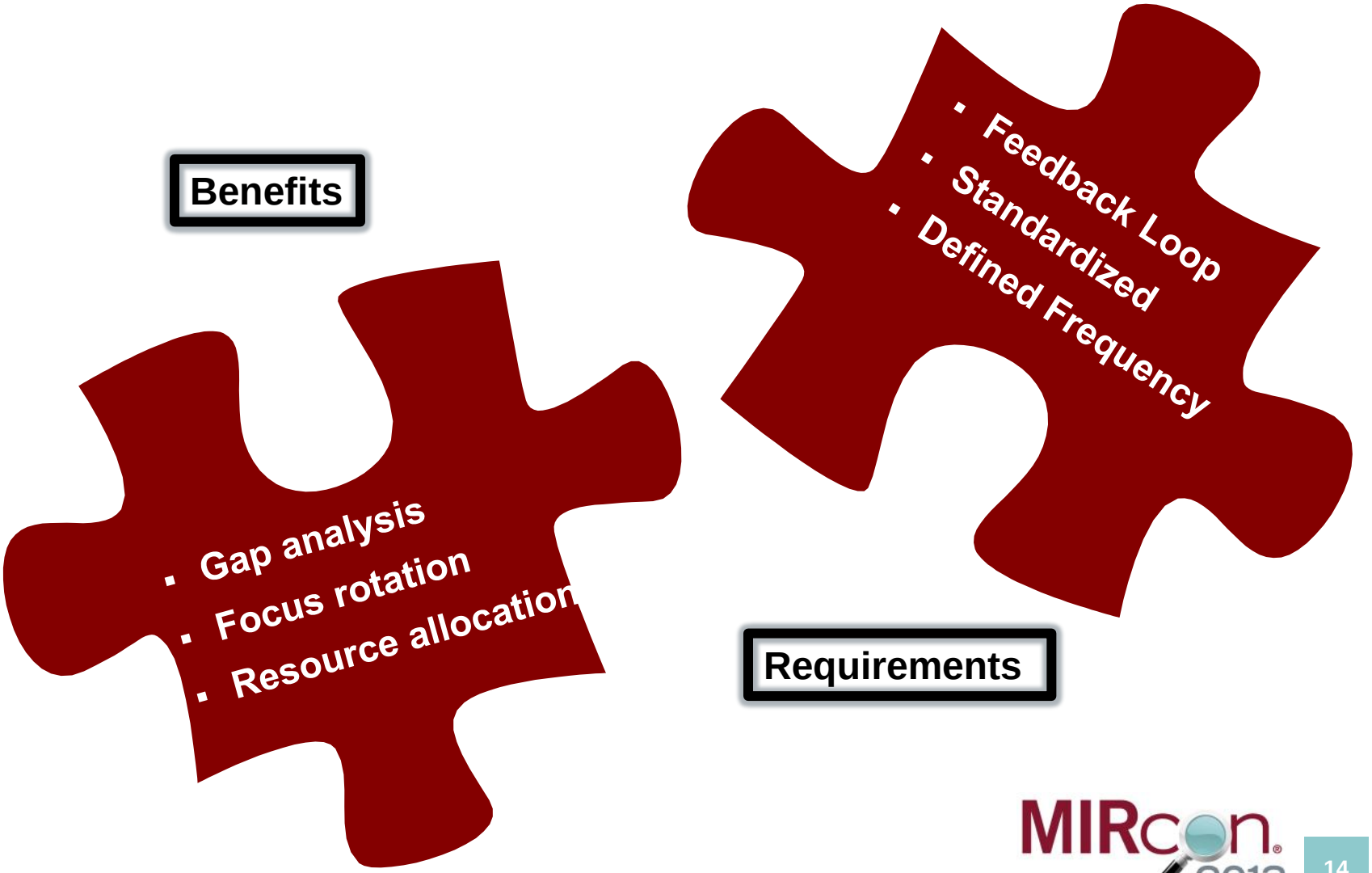
Field	Data
Metric	01 - Time to Detect
Reference Document	ACME SOP XYZ
Goal	Find the threat faster
Measure	Average hours to detect an incident from the moment of initial compromise
Formula	X = (Time to detect incident 1 + time to detect incident 2 + … time to detect incident n)/n
Objective	X < 8 hours
Frequency	Collection: Quarterly Reporting: Quarterly
Trend Retention	Three years
Responsible Stakeholder	SOC Manager
Data Source	Ticket system / Incident Reports
Reporting Format	Line Graph
Dissemination Mechanism	SOC Biannual Update

Reporting

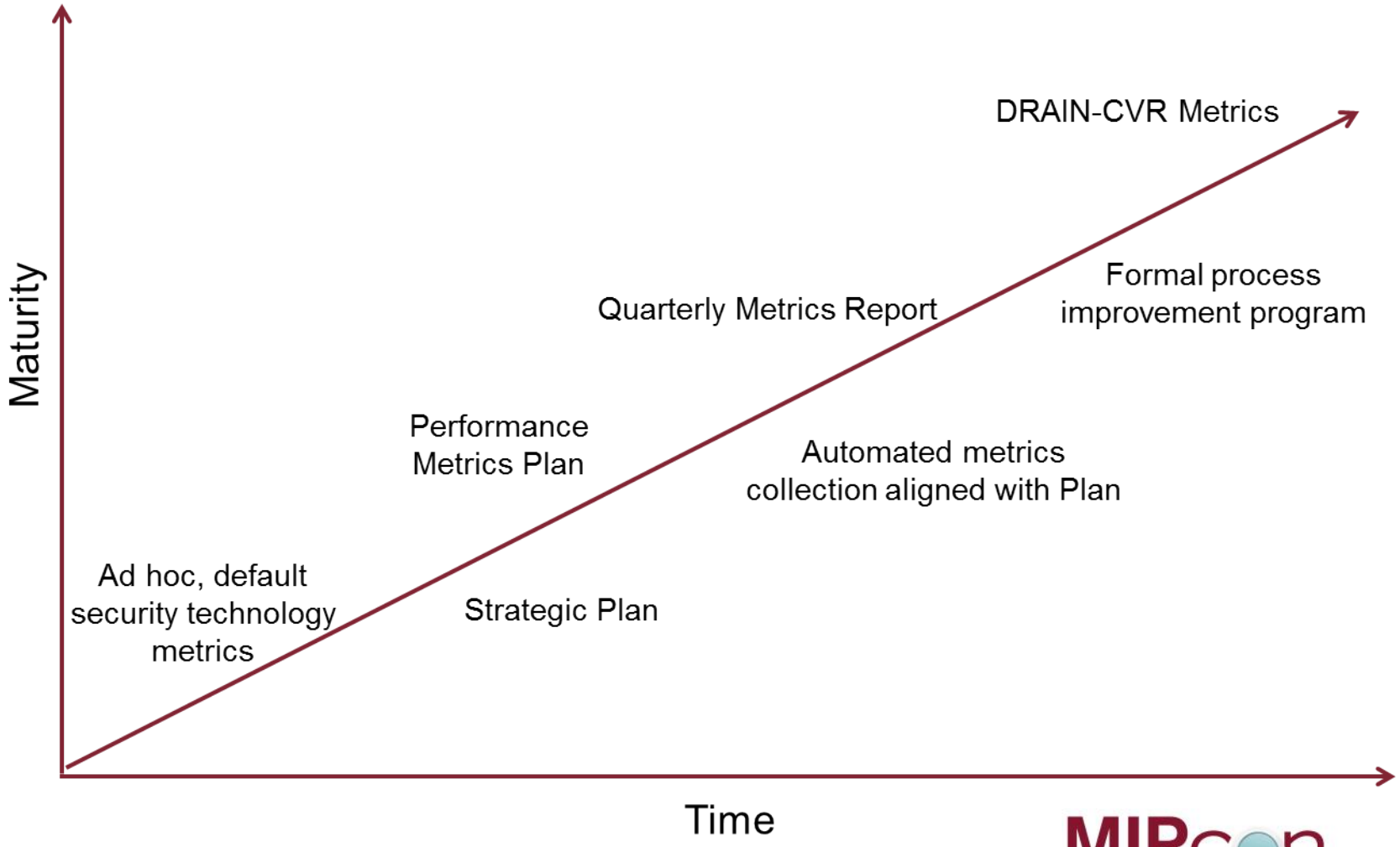
- Identify the appropriate audience
- Internal collection and external reporting may not adhere to the same frequency
- Report per-unit metrics where possible



Process Improvement



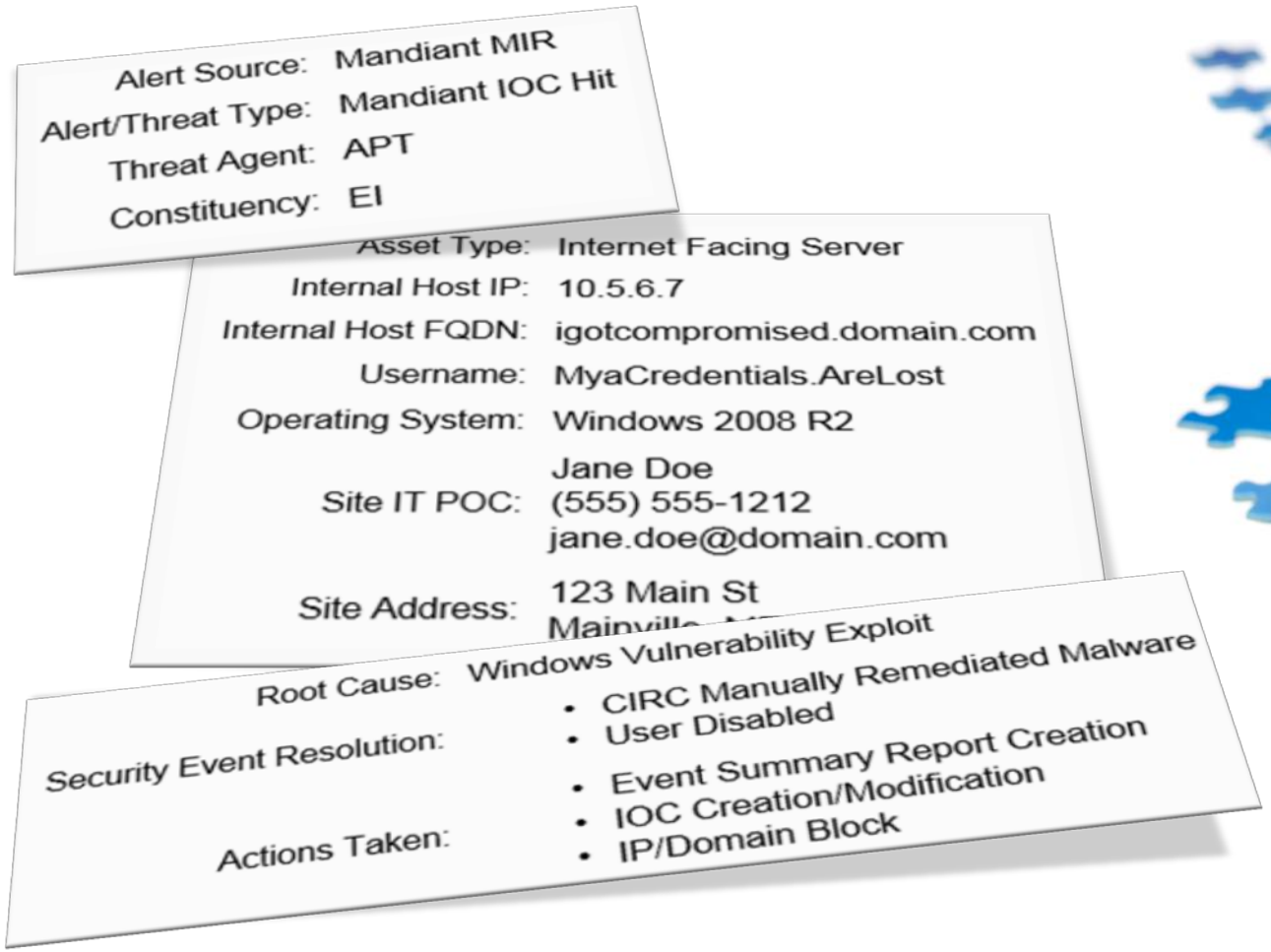
Key Milestones - Metrics

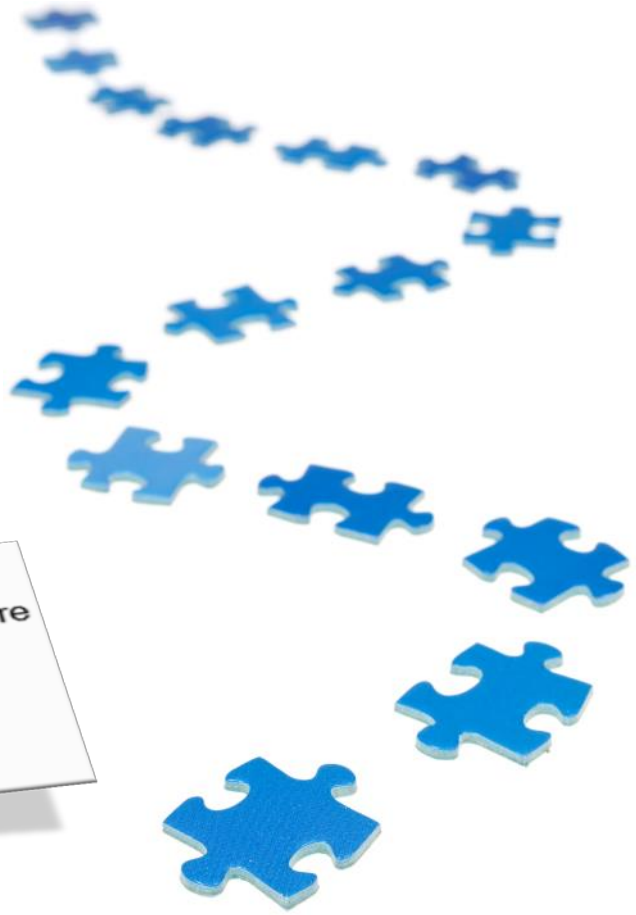


Practical Application – Lessons Learned

- Open-minded communication
- Centralized documentation
- Maintain perspective
- Don’t wait for perfect

Security Event Instrumentation

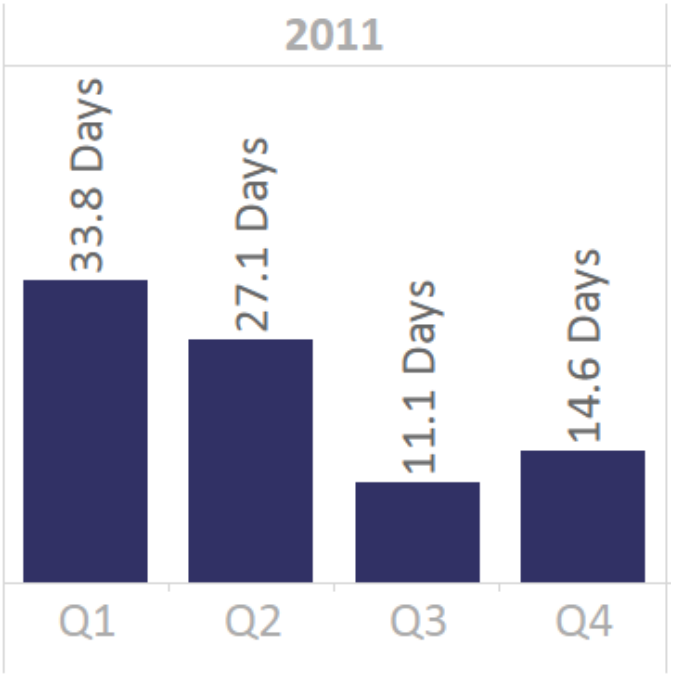




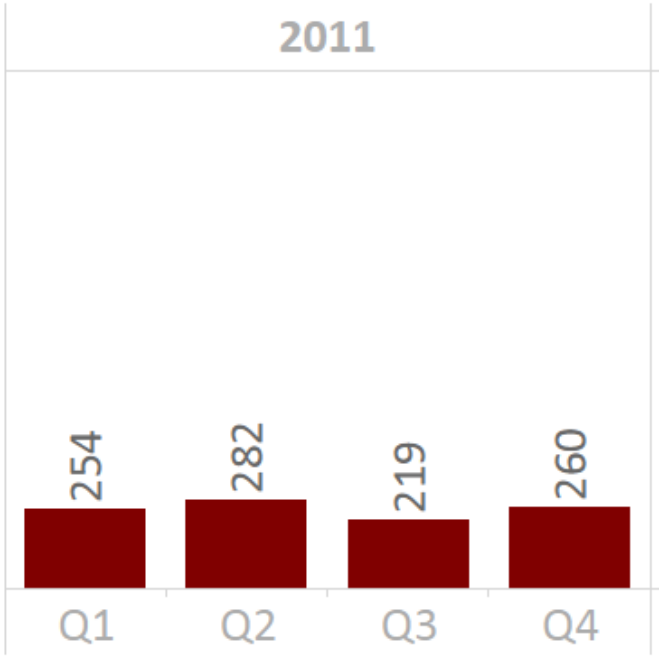
Action Request Instrumentation

Getting Started - The First Year*

Time to Resolve (TTR)



Security Event Volume

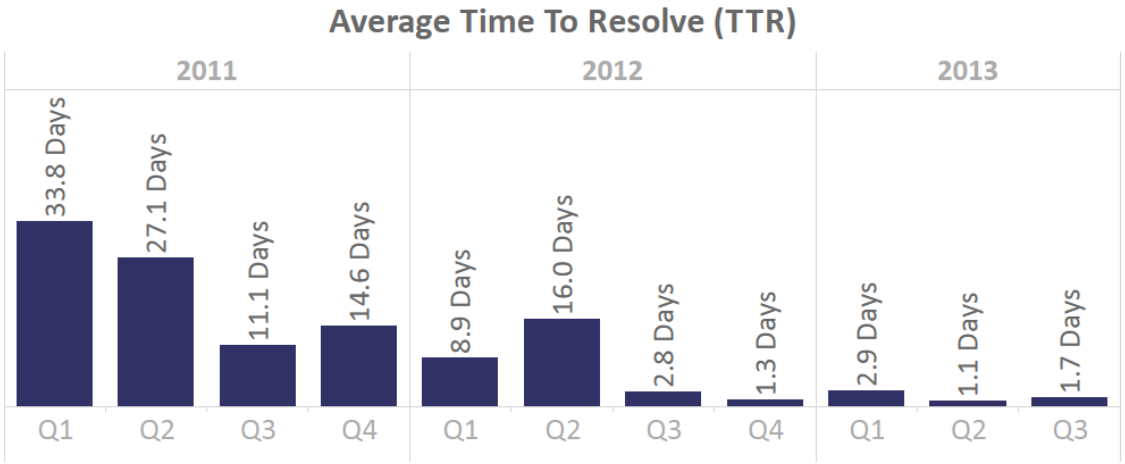


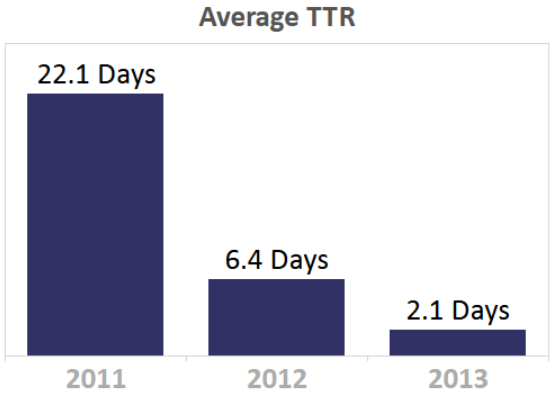
** Fictitious values with representative distributions*

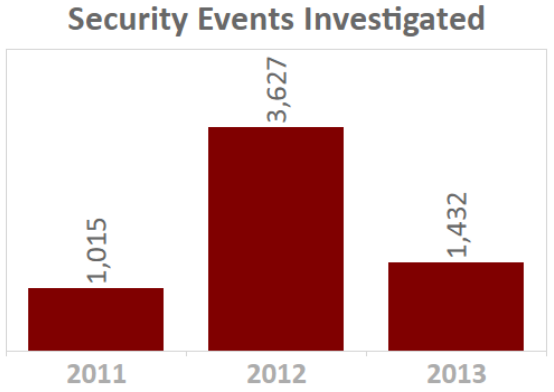
Process Optimization Examples

- Initial Event Documentation
  - 15min ➡ 5min or automated
- Asset Identification
  - 5min ➡ automated
- Evidence Collection
  - 30min ➡ 1min
- Metrics Data Collection
  - Ad-hoc ➡ automated
- Threat Correlation
  - Ad-hoc ➡ 1min

Continuous IR and Security Optimization*



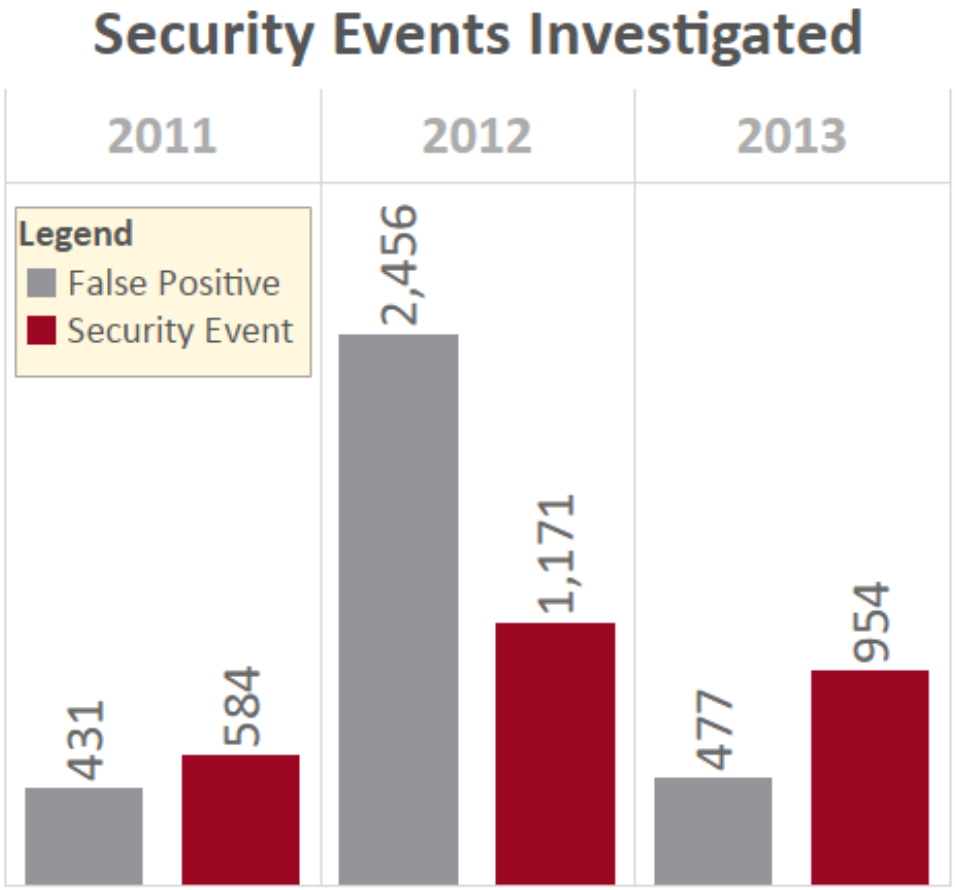


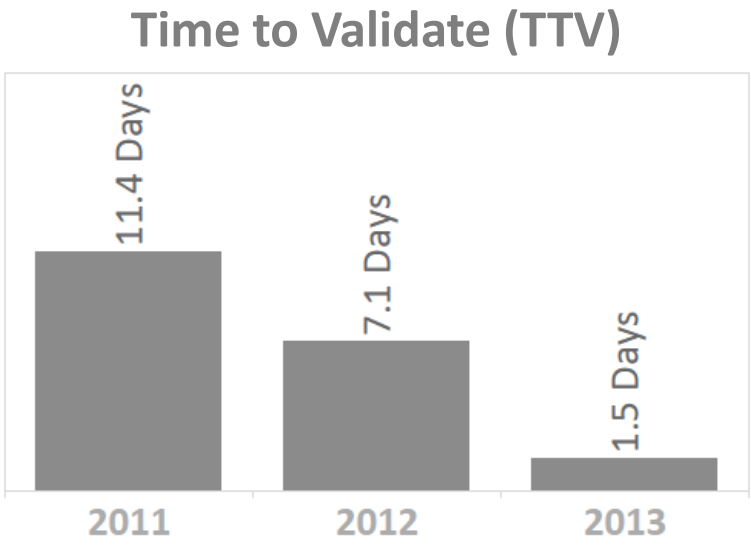


** Fictitious values with representative distributions*

MIRcon 2013

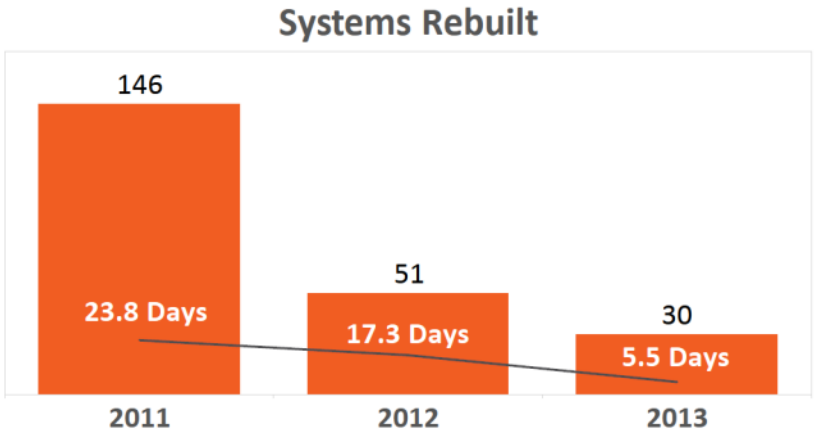
Time to Validate (TTV) *

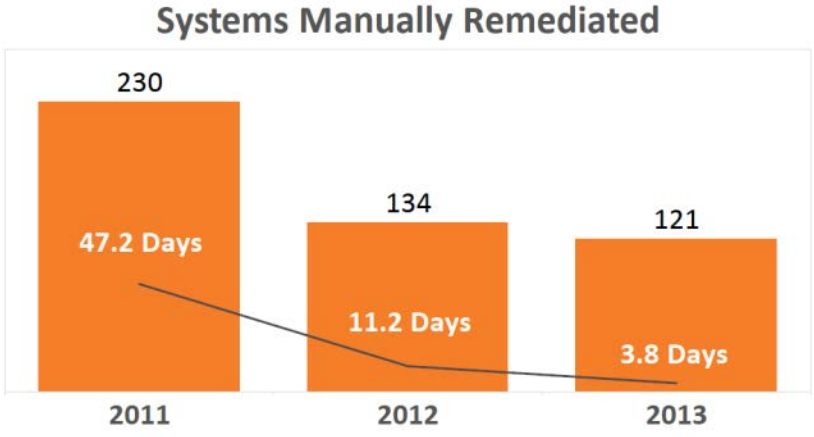


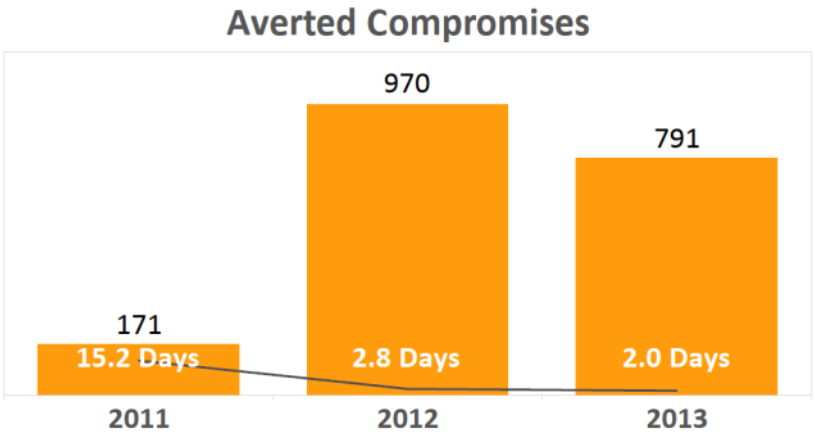


** Fictitious values with representative distributions*

Remediation Method and Time to React*



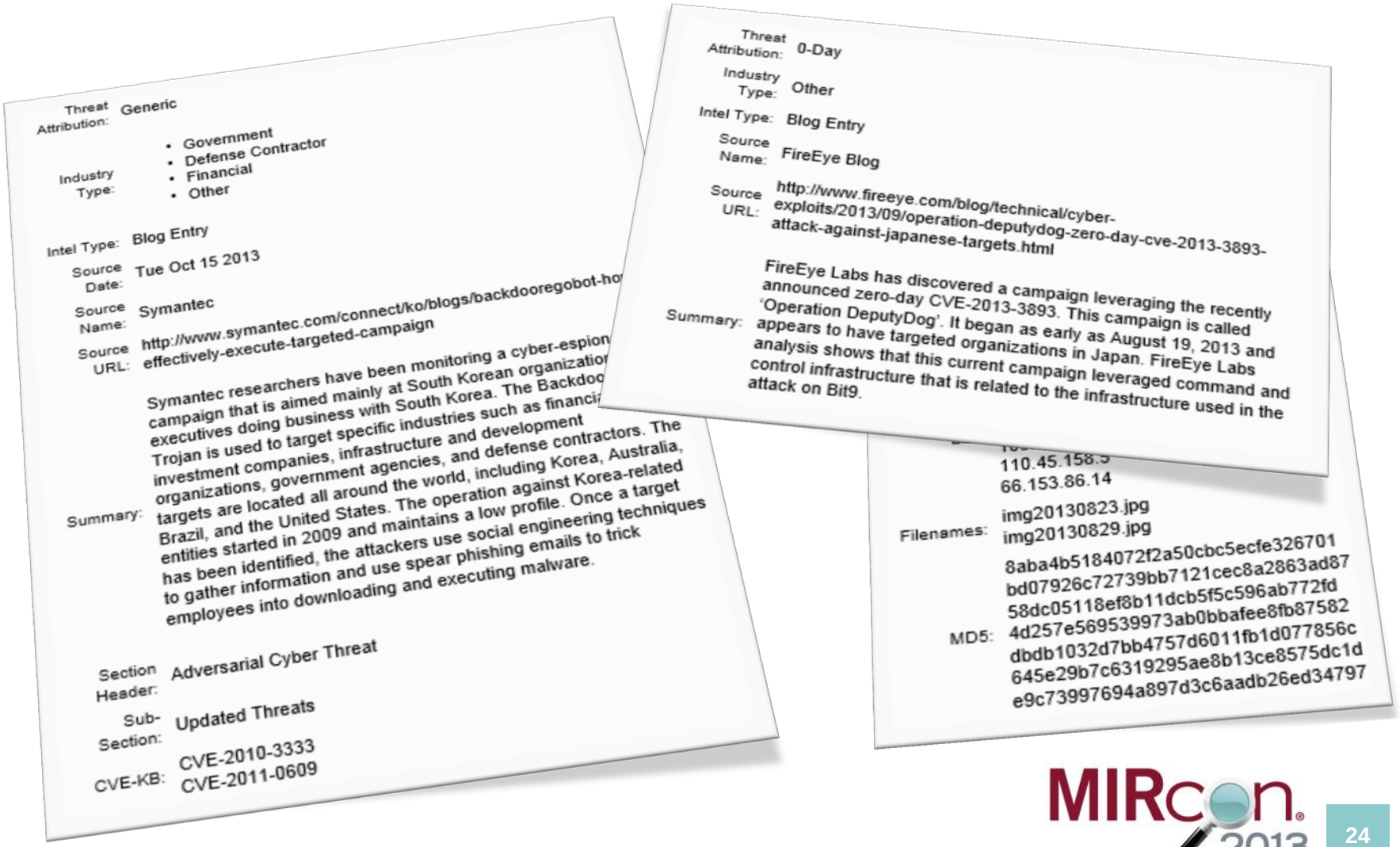




** Fictitious values with representative distributions*

MIRcon 2013

Threat Intelligence Integration



Threat Attribution: Generic

Industry Type:
- Government
- Defense Contractor
- Financial
- Other

Intel Type: Blog Entry

Source Date: Tue Oct 15 2013

Source Name: Symantec

Source URL: http://www.symantec.com/connect/ko/blogs/backdooregobot-ho
effectively-execute-targeted-campaign

Summary: Symantec researchers have been monitoring a cyber-espion
campaign that is aimed mainly at South Korean organizatio
executives doing business with South Korea. The Backdoo
Trojan is used to target specific industries such as financi
investment companies, infrastructure and development
organizations, government agencies, and defense contractors. The
targets are located all around the world, including Korea, Australia,
Brazil, and the United States. The operation against Korea-related
entities started in 2009 and maintains a low profile. Once a target
has been identified, the attackers use social engineering techniques
to gather information and use spear phishing emails to trick
employees into downloading and executing malware.

Section Header: Adversarial Cyber Threat

Sub-Section: Updated Threats

CVE-KB: CVE-2010-3333
CVE-2011-0609

Threat Attribution: 0-Day

Industry Type: Other

Intel Type: Blog Entry

Source Name: FireEye Blog

Source URL: http://www.fireeye.com/blog/technical/cyber-exploits/2013/09/operation-deputydog-zero-day-cve-2013-3893-attack-against-japanese-targets.html

Summary: FireEye Labs has discovered a campaign leveraging the recently announced zero-day CVE-2013-3893. This campaign is called 'Operation DeputyDog'. It began as early as August 19, 2013 and appears to have targeted organizations in Japan. FireEye Labs analysis shows that this current campaign leveraged command and control infrastructure that is related to the infrastructure used in the attack on Bit9.

110.45.158.5
66.153.86.14

Filenames: img20130823.jpg
img20130829.jpg

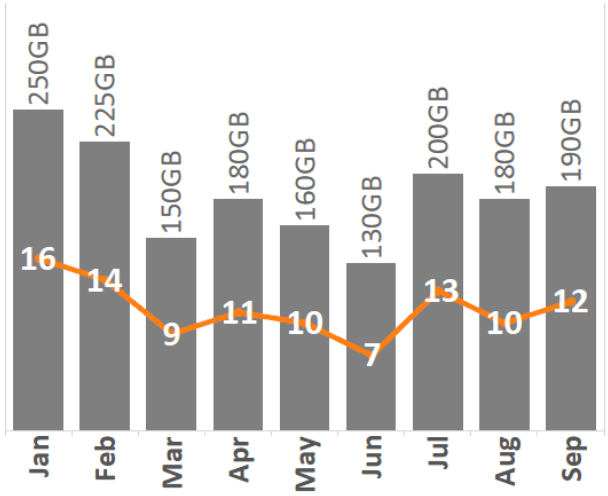
MD5: 8aba4b5184072f2a50cbc5ecfe326701
bd07926c72739bb7121cec8a2863ad87
58dc05118ef8b11dcb5f5c596ab772fd
4d257e569539973ab0bbafee8fb87582
dbdb1032d7bb4757d6011fb1d077856c
645e29b7c6319295ae8b13ce8575dc1d
e9c73997694a897d3c6aadb26ed34797

Reporting – Lessons Learned

- Defined and consistent:
  - Schedule
  - Scope
  - Structure
- Content
  - Concise and high level
  - Map to areas of interest
  - Address concerns and fears
  - Maintain business context
  - Educate and inform

Point-in-Time Reporting and Metrics*

Non-Corporate Webmail Traffic Volume vs. Security Events

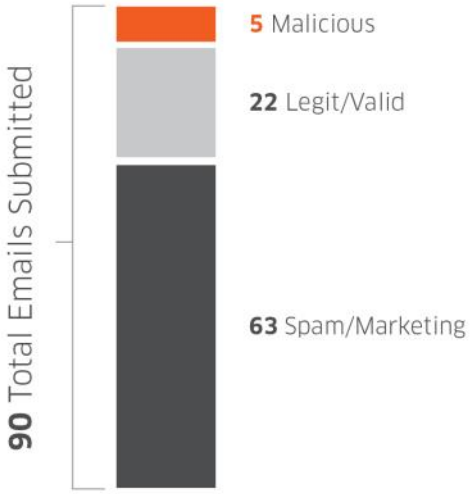


OUTBOUND NETWORK TRAFFIC

Top 10 Destination Countries

United States	95.24%
Ireland	1.09%
Canada	0.94%
United Kingdom	0.66%
Sweden	0.48%
Australia	0.44%
France	0.26%
Germany	0.18%
Qatar	0.16%
Netherlands	0.09%

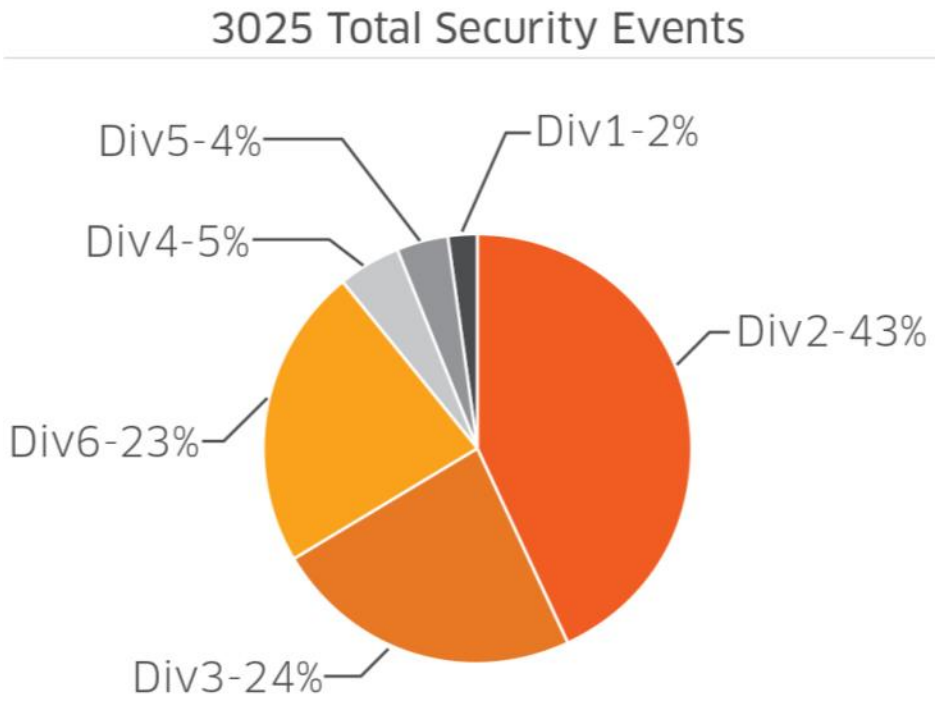
Reported Email Threat Determination



** Fictitious values with representative distributions*

MIRcon 2013

Executive Reporting Examples*



20% of security events are a result of **targeted and/or malicious phishing attacks.**

12% of security events are a result of **undetected malware or other forms of compromise.**

Saved **$150k+*** in 2012
by avoided labor costs due to advanced remediation techniques
*(8hrs IT Labor + 8hrs Lost Productivity) x $100/hr per system

** Fictitious values*

MIRcon 2013

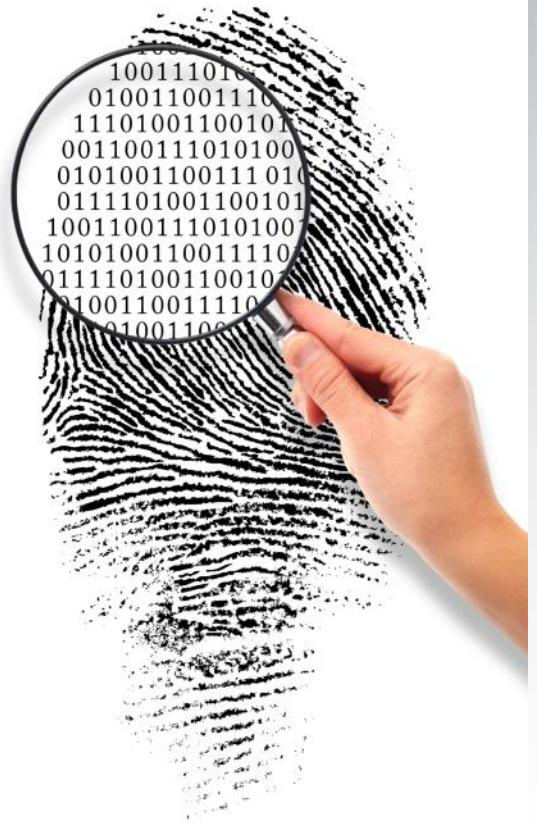
Questions

Joshua Bartolomie
Director | Exelis Cyber Security Operations
joshua.bartolomie@exelisinc.com

Matthew Shaffer
Consultant | Mandiant Strategic Solutions
matthew.shaffer@mandiant.com

Appendix:
Example Security Event Data Points

- Event Data*
  - Alert Source**
  - Alert/Threat Type**
  - Constituency**
  - Asset Type**
  - Internal Host IP
  - Internal Host FQDN
  - Asset OS**
  - Threat Agent**
  - Threat Domains/IPs
  - Actions Taken**
  - Root Cause**
  - Resolution**
  - Targeted Attack**
  - Username
- Action Requests*
  - Evidence Collection**
  - Software Install/Upgrade**
  - Incident Reporting**
  - Analysis Assistance**
  - Malware Analysis**
  - Malware Submission
  - Network Block
  - Network Capture
  - Request Approval**



* Use a single record per individual unit of interest

** Predefined selections to ensure standardization